

## 4. Map vulnerabilities, find hidden flags!

---

**Time to map out vulnerabilities with nmap! Can you sneak past our defenses and unearth those open ports?**

Welcome to the next level of your cybersecurity adventure! We're taking our Asset Discovery tool up a notch by integrating nmap for open port checks. But have we secured it enough

`Nmap Time`! Ready for a New Challenge? 🕵️

This challenge focuses on exploiting a command injection vulnerability within the nmap input.

- Target Application: [Asset Discovery tool](#)
- Initial Endpoint: `http://web0x09.hbtn/app5/`

---

Useful instructions:

1. Log into Asset Discovery tool.
2. The nmap input `is` vulnerable.
3. We can `try` and give it an input (`127.0.0.1:3000` for example).
4. Flag Location `/bin/4-flag.txt`